Did You Forget Your Password?

Abbas Moallem

San Jose State University
Abbas.moallem@sjsu.edu

Abstract. A quantitative research surveying 390 people with different levels of expertise in computer usage was conducted to understand user behavior from three perspectives: How users make sure that the sites they are using are safe, How users deal with forgotten passwords, How secure is the "security questions". The finding shows users' pattern of behavior in checking security when viewing a web application, the way they deal with numerous passwords and retrieval of the forgotten password by using the security question. The research concludes that most people would be able to answer a variety of security questions for other people in their entourage. Users seem to have significantly different behaviors statistically by age group and level of expertise.

Keywords: Password, Authentication, Security, Reset Password, Password Remembrance, eCommerce.

1 Introduction

Accessing web applications is now part of every individual's daily life. According to internetworldstats.com, nearly 1.9 billion people use the Internet to log into bank accounts or ecommerce to manage their finances or order goods, send and receive emails, or socialize through networking and community sites several times per day.

To access the right location users must point their browser to the right location (the page) and then authenticate themselves with a user ID and password. This process is not as straightforward as it appears.

The first question one might ask is how can users go to a specific web application or website and check if it is really the location that they intended to go to and not a fraudulent one. Users might use different methods to access a specific location. These methods might be typing the URL or domain name in the address bar, using a saved bookmark, or simply clicking a link from another page. The use of any of these methods might require a different effort from the user's perspective, but all also represent risks. For example a slight misspelling when the user enters the domain name into the address bar as well as a misleading link might take the user to a fraudulent site and easily acquire the user's authentication information (Keats, 2007, Edlerman, 2008).

Fraudulently acquiring people's sensitive information such as user ID, passwords, and credit card details through a deceitful link usually by e-mail or instant messaging (known as phishing) is widely known and documented security issue. However, many people still might click on the deceptive link and enter their private information. Researchers report a

A. Marcus (Ed.): Design, User Experience, and Usability, Pt II, HCII 2011, LNCS 6770, pp. 29–39, 2011.

variety of techniques to use web history to access users' information (Naone, 2010, Jagatic et al, 2005, CIO Council, 2009, Castelluccia et al, 2010).

The second question is how would users check to see if the site is using a safe connection or is not a phishing site or parking page? To check the validity of a site, a variety of methods were offered, in this case the most common techniques for validating the site, by the order of best security offered are: checking external certificates, checking connection HTTPS, checking site reputation by looking at the appearance and content of the site or rely on third-party applications to check the validity of the visited site.

Among all of the above checking an external certificate seemed to be the most reliable method. Although this method seems to be the most reliable checking method, it is still not 100 percent secure since the hacker can for example go to the user's computer and change the list of certificate authorities to make it trust an un-trusted certificate authority.

Checking the HTTPS connection, which is also related to the certificate validation, is another reliable method to check the validity of a web application site. The main idea of HTTPS is to create a secure channel over an insecure network. An HTTPS connection uses certificates to validate trusted authorities. If that check fails, then the browser will warn users. However some research suggests that site-authentication images are ineffective and the users do not withheld their passwords even when the site is not using the HTTPS connection (Schechter et al. 2007).

Another method to check the validity of a site is by paying attention to the look and content of the site but this method alone would not be a reliable security check. Most of the phishing sites simulate a total visual replica of the original site.

A further technique to check the security of the site visited is to rely on third-party applications. These applications check the validity of the visited site and inform the user about the site. Despite their use of safety features, they require the users to have a basic understanding of Internet security features and the risks and notifications or warnings offered by these applications.

The next step is for the user to pass the authentication phase. This process consists of authenticating users through the use of one or more of three "factors" (FFIEC, 2008): something the user knows (e.g., password), something the user has (e.g., smart card); or something the user is (e.g., fingerprint).

Among these factors the authentication through user ID (or user name) and password seems to be the most common one.

With accumulations of the web application accounts, users' behavior was the subject of a variety of studies that include: the diversity of the password format requirements, too-easy-to-guess passwords and methods to prevent dictionary attacks, number of password that each user uses to access different accounts, password complexity, difficulty to remember passwords and user names for different account, self-resetting password, and password retrieval. (Florencio & Herley, 2007, Gaw & Felten , 2006, Englert & Shah, 2009, Forget & Biddle, 2008, Karaca & Levi, 2008, Weir et al, 2010).

According to research cited above, users do not seem to be very conscious about the security issues or do not take into consideration the reliable cues. Users use a limited number of passwords that are sometimes very simple if they are not forced by password policies to make their password more complicated. The users may have many web accounts but that does not mean they have different passwords for each account.

To improve security, web applications now use several features to address forgotten passwords and ID reset. These functionalities consist of providing a user with a self-reset password and user ID capability requiring them to answer several security questions, and then, if the answers are correct, the passwords are sent through email to the email address on file. Then the user must use that temporary link or password to login and change their password.

Despite the various studies reviewed above, there seem to have been no studies that have been conducted from the perspective this study uses.

Consequently this research tries to answer the following questions:

- How conscious are users about the security when they login to a web application?
- How do they check if the site is secure?
- How often do they use password or user name reset features?
- How much security is offered by security questions in these reset features?

We have considered two parameters that might be distinctive among the users: age and expertise. We hypothesized that younger and more expert users might have a different behavior in all the above factors.

2 Methods

An online survey was designed containing three groups of questions: questions regarding respondent profile, security, and forgotten password reset features and security questions.

A message, with a link to online surveys, then was sent to LinkedIn groups, investigator's former students, and posted online in several groups to voluntary participants to take the survey. A total of 390 responses were collected. All data was collected from mid- March, to mid- May 2010. The data collected through this survey was then analyzed using statistical analysis.

Participants. Overall 64% of the respondents were male and 36% female. The percentage of the respondents by age group is: 41% over 55, 21% 46-55, 32%, 36-45, 25%, 26-35 and 9%, 18-25. 57% of participants have a graduate school level of formal education and 34% a college degree. The participants were asked to self-evaluate their level of expertise in computer usage. 34% evaluated their expertise as Expert, 45% as Advanced, 20% as Intermediate.

3 Results

In this section we will review responses collected for each group of questions: Security, Forgot password and Security Questions.

3.1 Security Questions

To understand the user behavior in checking the security of a site, 3 questions were asked. In the following section, we will analyze the answers provided to these questions.

Q-S1: How do you find the site you intend to log into?
Overall 62% of the responses indicate that participants type the URL address in the address bar, 59% use their bookmarks, and 36% use search. Typing the URL into the address bar seems to be favored more by "expert" users. However, older participants seem to favor using bookmarks 72% among the over 55 age and 73% among age 46-55 but 52% among the 26-35 age group.

Q-S2: Once you get to the site that you have requested, how do you make sure that the displayed site is a real site and not a fake or fraudulent site?
Overall the look of the application is the primarily checked option (51%) followed by checking browser certificate validation (43%). It is also interesting to observe that 13% of the participants declare not being aware of any of the suggested techniques for checking the validity of the site. Only 18% of the respondents use a third-party application to check the validity of the site.

Looking at this data shows that checking the browser certificate validation seems to be used more among the expert users (62%). Overall it seems that the main way to check validity of the web application site is the look of the site even among the expert users (41%). Interestingly, 12% of self-evaluated advanced user and 7% of expert users declare not being aware of any method to check the validity of the site.

The data analysis by age group reveals that the age group of 36-45 and 46-55 use more advanced validation methods such as external or browser certificate validation. Overall users seem to rely more on the look than on the use of advanced validation techniques such as certificate valuation.

Q-S3: Whenever you are entering your personal information on an Internet site such as a bank ecommerce or registration page, how do you know if the site is secure and that you have a secure connection?
The participants could select one or more options in the list. The results show that considering all participant answers 64% say they rely on HTTPS, 44% SSL lock, 43% say they use only sites with known reputations or they rely on VeriSign or similar logos (22%).

Looking at the data by self-evaluated level of expertise reveals that reliance on HTTPS and domain name raises by user's level of expertise. For example, fewer intermediate users (27%) check HTTPS versus expert users (82%) or check domain name (63%) among the expert users versus (30%) intermediate users.

3.2 Forgot Password

To understand the user behavior in password retrieval, seven questions were asked of the participants. In the following section, we are analyzing the answers provided given to these questions.

Q-P1: Overall how many different passwords do you use to log in to different web applications or websites?

The results indicate that a negligible number of people use one password. 7% use only two passwords but 49% of the respondents use three to five passwords. Users belonging to the self-evaluated "expert level" seem to use more passwords 48% of use more than 5 passwords. It seems that people with a lower level of expertise use fewer passwords than users with a higher level of expertise. Analyzing the results by age group reveals that older users use more than 5 passwords (over 55 age, 54% and age 26-36 42%). Considering all results, it seems that almost the same ratio of people (33% to 57%) across the expertise and age groups use three to five passwords.

Q-P2: How often do you forget your password to log into an application such as a bank account that you use often and for which your user ID and password are not already saved by the browsers?

22% declare they never forget their password for the frequently used application, 51% seldom, and 23% sometimes.

Q-P3: How often do you forget your password to login to an application that you use rarely and your user name and password are not already saved?
The results show that 35% of the respondents often forget their password and 39% sometimes forget. Interestingly 4% of respondents never forget their password. It seems that older users forget their password more often. 32% of people among age group 26-35 forget their password sometime versus 50% among 46-55 age group. However, the decline in the forget rate for the age group of over 55 is 31%, which might indicate that users keep a record of their passwords.

Q-P4: How often do you use the forgot password feature to reset or find your password or user ID/name for applications you use rarely?
The results show 64% of participants seldom use the reset password feature versus 5-to 6% percent every time or often.

Q-P5: Which of the following methods do you like the best to find your user name or password?
The results show that 41% of the participants prefer to answer security questions and receive their password or reset link by email. 26% prefer to answer security questions and then immediately reset the password, 32% prefer to click forgot password/user ID, enter and receive reset password link by email, and almost nobody wants to call support for resetting their password. However, preference for clicking forgot password/user ID, enter and receive reset password link by email is stronger among younger age groups and experts (26-36, 38%, 36-46, 37%, and expert group 42%).

Q-P6: How often do you customize the security question to find your password?
The results shows 25% often customize the question, 28% never do, and 45% sometimes do. The percentage is higher among the more advanced users quite often, 33%, sometimes 39%, but not necessarily different among the age groups.

Q-P7: Do you use any 3rd party application or hardware to store your password and login information?
Overall 70% do not use any third-party software is higher among more expert users (Expert group 48%) but seems not much different among the age groups.

3.3 Security Questions

The participants were asked to estimate the number of people for whom they might know the answers to the questions that are generally asked during user ID and password reset. (Table 1)

Table 1. Security Questions List

For how many people can you answer the following questions?	
In what city was he/she born?	What was his/her first job title?
What is the name of his/her first pet?	What brand was his/her first car?
What is the name of the first company he/she worked for?	What is the name of his/her pet?
What is the name of his/her mother's maiden name?	What is his/her favorite teacher?
What is the name of his/her paternal grandmother?	What color was his/her first car?
What is the name of his/her closest friend at high school?	What color is his/her favorite color?
What was his/her favorite subject in high school?	
What is the name of his/her childhood best friend?	

The results show that for most of these common password reset questions participants know the answer for one or many persons. The more general questions such as in “What city you were born?” only a negligible fraction of people (1%) did not know anybody else’s place of birth. Fewer people knew the answers to questions that required older memory information such as, “your favorite teacher”. 51% did not know anybody’s information about favorite teacher. Even for this question 49% knew at least information about one person. (Figure 1)

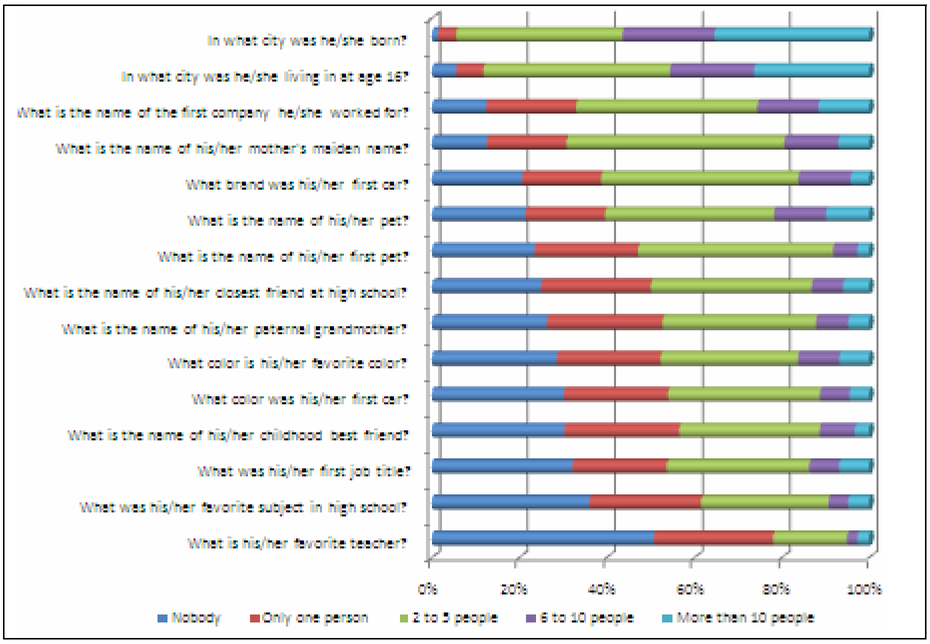

Fig. 1. For how many people can you answer the following questions?

4 Analysis

Statistical data analysis using ANOVA single factor was performed to identify whether there is any significant differences among the groups of participants based on age or level of expertise to verify the following hypotheses.

Participants significantly differ on how they check the security of a web application based on their Age group and level of expertise.

The ANOVA test results indicate no significant differences between the different age groups for questions S1, S2, P3, P6, and P7. The ANOVA reveals significant differences for questions P1, P2, P4 and 5. P-values are 0.69. 0.60 0.75 and 0.53 (Table 2).

The ANOVA test results indicate no significant differences between the different levels of expertise levels for questions S1, S2, S3 and P2, P3, P5 and P6. The ANOVA reveals significant differences for questions P1, P4 and P7. P-values are 0.58., 0.65, and 0.58.

A significant difference was also noticeable between and within age groups for Question P5 and for Question P7 between and within groups based on level of expertise. (Table 3)

This result tends to indicate that the subjects have different behavior in the number of passwords based on different age groups and level of expertise. This seems to be the same for the number of passwords and how often they use the forget password for web applications they rarely use.

Table 2. ANOVAs Single Factor Test Result –Age Groups: 26-35, 36-45, 46-55 & Over 55

Question	Source of Variation	SS	df	MS	F	P-value	F crit
P1	Between Groups	600.4	3	200.13	0.49	**0.69**	3.23
	Within Groups	6490.8	16	405.67			
	Total	7091.2	19				
P2	Between Groups	600.4	3	200.13	0.63	**0.60**	3.2
	Within Groups	5044.8	16	315.03			
	Total	5645.2	19				
P4	Between Groups	600.4	13	200.13	0.40	**0.75**	3.2
	Within Groups	7914.8	16	494.75			
	Total	8515.2	19				
P5	Between Groups	600.4	3	200.13	0.76	**0.53**	3.2
	Within Groups	4190.8	16	262.92			
	Total	4791.2	19				

The participants seem to prefer typing a URL or using a bookmark to navigate to the desired web application site. The results also suggest that advanced and expert users tend to prefer typing the URL whereas older users tend to prefer bookmarks. This might be related to ease of typing and movements as younger users might have more rapid text entry skills than older adults. Research associates aging with changes in motor skills, including slower response times, decline in ability to maintain continuous movements, distribution in coordination, loss of flexibility, and greater variability in movements (Rogers & Fisk, 2000).

Table 3. ANOVAs Single Factor Test Result - Level of Expertise: Intermediate, Advanced, & Experts

Question	Source of Variation	SS	df	MS	F	P-value	F crit
P1	Between Groups	950.53	2	475.26	0.55	**0.58**	3.88
	Within Groups	10234.4	12	852.86			
	Total	11184.93	14				
P4	Between Groups	650.53	2	475.26	0.44	**0.65**	3.88
	Within Groups	12770.4	12	1064.2			
	Total	13720.93	14				
P7	Between Groups	2376.33	2	1188.16	0.64	**0.58**	3.88
	Within Groups	5505	3	1835			
	Total	7881.33	5				

The results of how participants ensure the site is a real site and they are not looking at a fake site suggests that no matter the age or level of expertise the primary verification seems to be the visual aspect of the site followed by browser certificates check. More advanced users tend to rely on external validation certificate check. The use of third-party validation is less than 20%. However according the New York Times (Helft M. 2010), the "number of such third-party "certificate authorities" has proliferated into hundreds spread across the world, it has become increasingly difficult to trust that those who issue the certificates are not misusing them to eavesdrop on the activities of Internet users, the security experts say".

The other most alarming factor is that 13% of participants declare they do not know any method to check the validity of a site. This number indicates the potential risk of these users to become victims of all types of fraud. The participants' comments indicate that some users experienced an invalid certificate for a valid site. This behavior makes users not really trust the browser validation test as one participant's comment indicated, "Certificates have proven to be worthless. Trusted sites have invalid certificates (even Microsoft at times!)." Many participants indicated visual verification of the URL as the primary check of the site validity. Or "according to the Electronic Frontier Foundation, more than 650 organizations can issue certificates that will be accepted by Microsoft's Internet Explorer and Mozilla's Firefox, the two most popular Web browsers. Some of these organizations are in countries like Russia and China, which are suspected of engaging in widespread surveillance of their citizens" (Helft M. 2010). In the Jones et al. (2007) study, it was also found that most respondents were unfamiliar with authentication technologies and suggested that though users are typically concerned about privacy and security, they do not necessarily understand how these issues are impacted by the use of digital identities.

On how a user knows if the site is secure and that they have a secure connection, the results are even more alarming. 6% of all participants indicated that they do not check anything at all. However, we observed a surprising 64% of users check to see if the site uses HTTPS 45% check the domain, 22% pay attention to third party validation such as VersiSign, 44% check the browser lock and 28% pay attention to security image. It seems that the younger group checks security less than the older group. Checking the security, according to Herley (2009), seems to have a direct relationship with the cost of an attack and greater indirect cost of effort by users.

These results are also consistent with other research on security indicating that users did not notice the change in validity of page images (Schechter et al. 2007)

On the remembrance of passwords and password retrieval, the results indicate that a negligible number of people use one password. 7% use only two passwords but 49% of the respondents use three to five passwords. Users belonging to the self-evaluated “expert level” seem to use more passwords 48% use more than 5 passwords. It seems that people with a lower level of expertise use fewer passwords than users with a higher level of expertise. Analyzing the results by age group reveals that older users use more than 5 passwords (over 55 age, 54% and age 26-36 42%). Considering all results, it seems that almost the same ratio of people (33% to 57%) across the expertise and age group use three to five passwords.

The low number of passwords generally used by users indicates that most users use the same category of passwords for several applications. Interestingly, the lower number of password retrieval among the older users group indicates that many users keep a written record of their password on paper. Writing down passwords has been reported by previous researchers (DeAlvare, 1998, Adams & Sasse 1999). DeAlvare reports that 50% of questionnaire respondents wrote their passwords down in one form or another.

An important percentage of the participants 22% declare they rarely use the passport retrieval for frequently used accounts and 27% seldom use it for not frequently used account. This might be another indication that users keep a written version of their password, or use the same password for most of their accounts. The higher percentage of users who rarely or seldom use re-set password, among the older age group, is supporting data and an indication of this behavior.

The findings of this study support the previous studies that a user who has more web applications does not necessary have more passwords. Consequently, it can be extrapolated that the users use the same password over and over for the types of accounts they use. Different password requirements for each application seems to be the main user issue since that would require users use the reset password. When applications require users to change their password frequently or will not allow the user use previously used passwords, this creates a huge usability issue for users.

All things considered, users still frequently use re-set password features and in this case the results support common sense that users do not like to contact customer support to reset a password. Around 25-29% of all ages and levels of expertise prefer to be able to re-set the password immediately with opening an email client to view the link or new temporary password. This percentage is higher (36%) among the over-55 age group.

Despite the fact that 41% of users like to answer the security questions and re-set their password (almost the same ratio among age groups and level of expertise), 28% percent of participants (26% to 30% among all age groups and level of expertise) declare that they never customize the security questions to find their password.

Participants seem neither to know nor to trust third-party software applications to manage their password. It seems more expert level users use a third-party application more often to manage their passwords. Considering that some password management applications seem themselves to be very insecure or users with multiple browses can’t take their password from one computer to another, it seems third-party software applications cannot resolve user password issues.

Consequently, answering the security questions seems to be offered often by application to retrieve the password or user ID/name. The common feature is answering a variety of preset questions. In the study, we were aiming to find out how many people were able to guess the answers to the security questions for someone else. This study shows that out of 15 typical security questions, even in the best case only 50% of people do not know the answers for somebody else in their entourage. Only the security questions that come more from the participant's episodic memory such as their favorite teacher or favorite subject in high school perform better. Consequently, there is a strong probability that somebody in a close one-person circle might get access to somebody else's accounts through family disputes, divorce cases, small partnership, and so on.

These results indicate that for Q-P1 "Overall how many different passwords do you use to log in to different web applications or websites?" the participants show a significant difference between and within groups based on both age and level of expertise.

5 Conclusions

The finding of this study supports previous studies in identifying the number of passwords and the security and degree of users' awareness, and concludes that most users are not aware of any way to check the security when viewing a web application. Many users use password retrieval by using the security question. However, most people would be able to answer a variety of security questions for other people in their entourage. People have a tendency to use a very small number of passwords, and they often keep track of those passwords most likely in paper format since a very strong percentage of people respond that they rarely use passport retrieval, especially among the older age group. Users know answers to the security questions of several people around them, and they might be able to answer them and get access to the password if they can get control of the email box.

Users seem to have significantly different behaviors in the number of different passwords they use to log in to different web applications or websites based of their age group and level of expertise. They also statistically differ by age group and level of expertise in the "reset password" feature frequency of use. Users are also differentiated by level of expertise in using 3rd party application or hardware to store password and login information. They are also set apart by age group in the methods used to find their user name or password.

This study needs to be expanded to a more diverse population so that more details of the behavior may be investigated through qualitative evaluation or each subgroup. The users' behavior in this field also evolves based on the user interface offered, but different web applications affect this tendency. Further research is needed to understand how users' behavior changes and to understand their needs and issues.

Acknowledgments. I would like to thank Mr. Mark Schertler, Security Architect at Axway, Inc. for his contributions to this study, Alice and Kenneth Kemp for editing the text, Shabnam and Nassim Moallem for their assistance in data collection and data exportation of this research.

References

[1] Adams, Sasse: Users Are Not the Enemy. Communications of the ACM(1999)

[2] Castelluccia, C.1., De Cristofaro, E., Perito, D.: Private Information Disclosure from Web Searches (The case of Google Web History) (2010), http://planete.inrialpes.fr/~ccastel/PAPERS/historio.pdf (accessed on September 23, 2010)

[3] CIO Council: Guidelines for Secure Use of Social Media by Federal Departments and Agencies, http://www.cio.gov/Documents/Guidelines_for_Secure_Use_Social_Media_v01-0.pdf (accessed on October 21, 2010)

[4] DeAlvare, A.M.: A framework for password selection. In: Proceedings of Unix Security Workshop II, Portland (August 29-30, 1998)

[5] Englert, B., Shah, P.: On the Design and Implementation of a secure Online Password Vault. In: ICHIT 2009, Daejeon, Korea, August 27-29 (2009)

[6] FFIEC, Federal Financial Institutions Examination Council: Authentication in an Internet Banking Environment (2005), accessed on http://www.ffiec.gov/pdf/authentication_guidance.pdf

[7] Forget, A., Biddle, R.: Memorability of Persuasive Passwords. In: CHI 2008 Proceedings, Florence, Italy. ACM, New York (2008) 978-1-60558-012-8/08/2005

[8] Gaw, S., Felten, E.W.: Password Management Strategies for Online Accounts. In: Symposium on Usable Privacy & Security (SOUPS), Pittsburgh, PA, USA, July 12-14 (2006)

[9] Helft, M.: Experts Warn of a Weak Link in the Security of Web Sites New York Times Published on (August 13, 2010), http://www.nytimes.com/2010/08/14/technology/14encrypt.html?_r=1 (accessed on August 23, 2010)

[10] Herley, A.: So Long, And No Thanks for the Externalities: The Rational Rejection of Security Advice by Users, Microsoft Research (2010)

[11] Jagatic, T., Johnson, N., et al.: Social Phishing. ACM, New York (2005), http://www.indiana.edu/~phishing/social-network-experiment/phishing-preprint.pdf (accessed on October 21, 2010)

[12] Jones, L.A., Antón, A.I., Earp, J.B.: Towards Understanding User Perceptions of Authentication Technologies. In: WPES 2007, Virginia, USA, October 29 (2007)

[13] Karaca, K., Levi, A.: Towards a Framework for Security Analysis of Multiple Password Schemes. In: EUROSEC 2008, Glasgow, Scotland, March 31 (2008)

[14] Keats, S.: Cashing in on Typos (2007), http://www.mcafee.com/us/security_insights/archived/oct_2008/si_oct5_08.html (accessed on May 19, 2010)

[15] Keats, S.: What's In A Name: The State of Typo-Squatting (2007), http://www.siteadvisor.com/studies/typo_squatters_nov2007.html (accessed on 05/19/2010)

[16] Naone E: Peeking Into Users' Web History, Technology Review (April 21, 2010), http://www.technologyreview.com/web/25159/?a=f

[17] Rogers, W.A., Fisk, A.D.: Human Factors, applied cognition and aging. In: Crailk, E.I.M., Salthouse, T.A. (eds.) The Handbook of Aging and Cognition. Lawrence Erlbaum Associates, Mahwah (2000)

[18] Schechte, S.E., Dhamija, R., Ozment, A., Fischer, I.: The Emperor's New Security Indicators. An evaluation of website authentication and the effect of role playing on usability studies. In: The 2007 IEEE Symposium on Security and Privacy, Oakland, California, May 20-23 (2007), accessed on http://usablesecurity.org/emperor